Defense Information Systems Agency

A Combat Support Agency

utomating STIGs: The Transition to CCI and SRG

DISA Field Security Operations
17 August 2011

DISA
A Combat Support Agency

Agenda

- What problems did we see?
- Automation of STIGs
- CCIs
- SRGs & Automation
- Future Direction
- Q&A

DISA
A Combat Support Agency

What Problems did we see ?

Secure Product Development

- No master list of all requirements for products
- Vendors do not know, in detail, what requirements they have to meet.
- Not knowing “when they are done”

IA Compliance Reporting

- Determining compliance statistics
- Inability to be able to validate that all requirements are addressed in current checklists
- Inconsistent reporting of findings and compliance status

Security Guide Development

- High Demand for New & Updated Security Guidance
- Duplication of requirements
- Vague / General guidance in DoD IA Controls
- Various interpretations of the requirements
- Requirements not written in a measurable format
- Inconsistency in documents from different sources
- Content Authors have to interpret the policies to determine what requirements they have to address. Not knowing “when they are done”

A Combat Support Agency

DISA Campaign Plan

Automating STIGs – Task 1.1.4.2.2.2

Title: Change the DISA Security Technical Implementation Guides (STIGs) so they are machine consumable and support automatic configuration management tools.

DISA
A Combat Support Agency

Our Way Ahead

CND Data Strategy and Security Content Automation Protocol (SCAP)

- ***A standards based approach to develop IA configuration guidance, publish IA guidance, assess assets, and report compliance***

- ***Benefits***
  - ***Enables vendor community to develop standardized guidance once for use by all communities***
  - ***Allow more commercial assessment tools to utilize DoD configuration guidance***
  - ***Requires less time to develop and publish additional guidance***

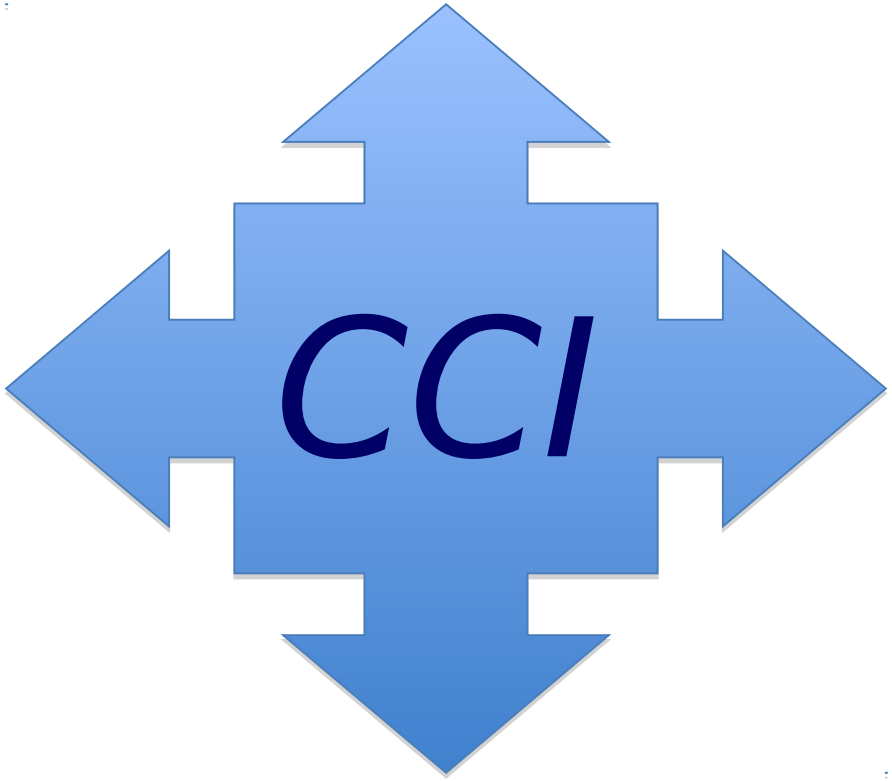
DISA
A Combat Support Agency

Transformation Progress

- **Combination of STIG and Checklist into a STIG that looks like a Checklist but has the authority of the STIG**
- **Publication of DoD Content (STIGs) in eXtensible Configuration Checklist Description Format (XCCDF)**
  - **XCCDF is an XML definition of a checklist**
  - **One of the NIST SCAP (protocols)**
- **Mapping STIGs to new DoD Control Set**
- **Breakdown of DoD Control Set into measurable Control Correlation Identifiers (CCI)**
- **Publication of automated benchmarks for use in SCAP tool (i.e., HBSS Policy Auditor)**

DISA
A Combat Support Agency

Control Correlation Identifiers (CCI)



A Combat Support Agency

First Phase CCI Creation

What is a Control Correlation Identifier (CCI)?

- Based on the NIST SP 800-53
- Decomposition of an IA Control or an IA industry best practice into single, actionable statements
- A foundational element of an IA policy or standard, written with a neutral position on an IA practice so as not to imply the specifics of the requirement
- Not specific to a product or a Common Platform Enumeration (CPE).
- CCI links requirements to policy – reduces ambiguity for consumers
- CCI should not require any changes to SCAP tools
- CCI used as a reference

The CCI List is:

- A collection of CCI Items, which express common IA practices or controls at the federal level

The CCI data specification is:

- Proposed to work in conjunction with the National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP)

Status of CCI

- Initial Draft list of CCIs complete
- Reference Security Requirements Guides to CCIs
- VMS changes to accommodate CCIs/SRG

DISA
A Combat Support Agency

CCI Use Cases

- **Secure Product Development**
  - Vendors can use CCI to incorporate security requirements into their products as part of the development cycle
  - They *'will know when they are done'*
- **IA Compliance Reporting**
  - CCI allows detailed reporting of compliance to IA Controls. Includes the ability to report partial compliance
- **Security Guide Development**
  - CCI data model in VMS will supports dynamic STIG generation based on asset characteristics
  - Supports Consistent Guide Development from External Sources

A Combat Support Agency

CCI Business Rules

A CCI must meet certain criteria to be considered a valid CCI.

- **Single requirement** – The CCI represents a single capability that was decomposed from the source policy document.
- **Actionable** – The CCI represents an action that can be taken against the system or an organizational policy.
- **Measurable** – The action that the CCI is describing will be something that can be determined or measured.

Example:

The organization manages information system authenticators for users and devices by establishing minimum password length requirements.

Decomposition of New Controls → Requirements

DISA
A Combat Support Agency

NIST SP 800-53v3

IA-5 AUTHENTICATOR MANAGEMENT

Control: The organization manages information system authenticators for users and devices by: Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; Establishing initial authenticator content for authenticators defined by the organization; Ensuring that authenticators have sufficient strength of mechanism for their intended use; Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; Changing default content of authenticators upon information system installation; Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*]; Protecting authenticator content from unauthorized disclosure and modification; and Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

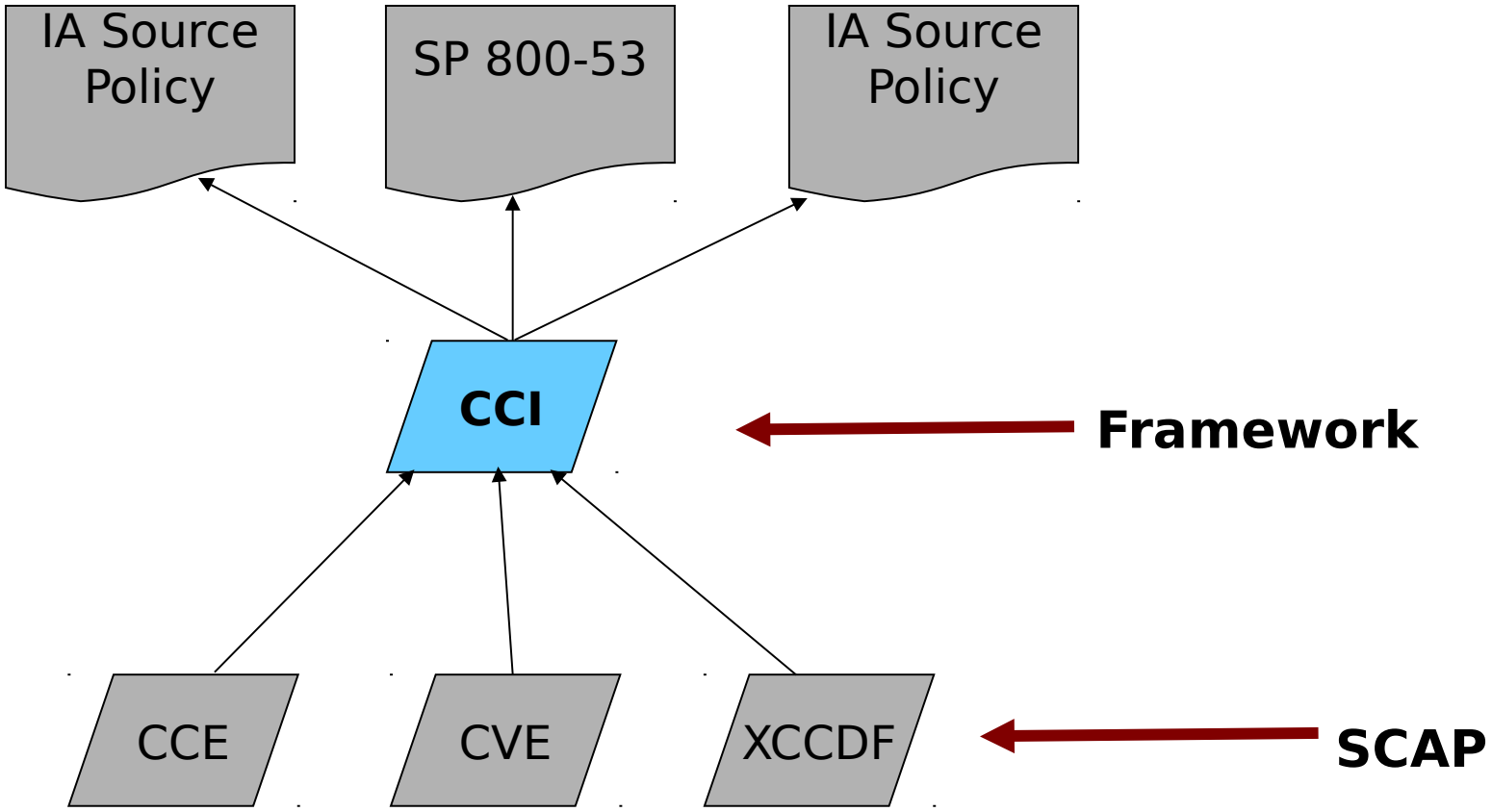
Control Correlation Identifiers

A decomposition of an IA Control or an IA industry best practice into single, actionable statements

CCI-000213: The organization enforces minimum password length.
CCI-000197: The organization enforces password complexity by the number of special characters used.
CCI-000188: The organization manages information system authenticators for users and devices by establishing the time period for changing/refreshing authenticators.
CCI-000186: The organization manages information system authenticators for users and devices by establishing maximum lifetime restrictions for authenticators (if appropriate).
CCI-xxxxxx: ……

DISA
A Combat Support Agency

CCI > Security Automation Our View



DISA
A Combat Support Agency

SRG

DISA
A Combat Support Agency

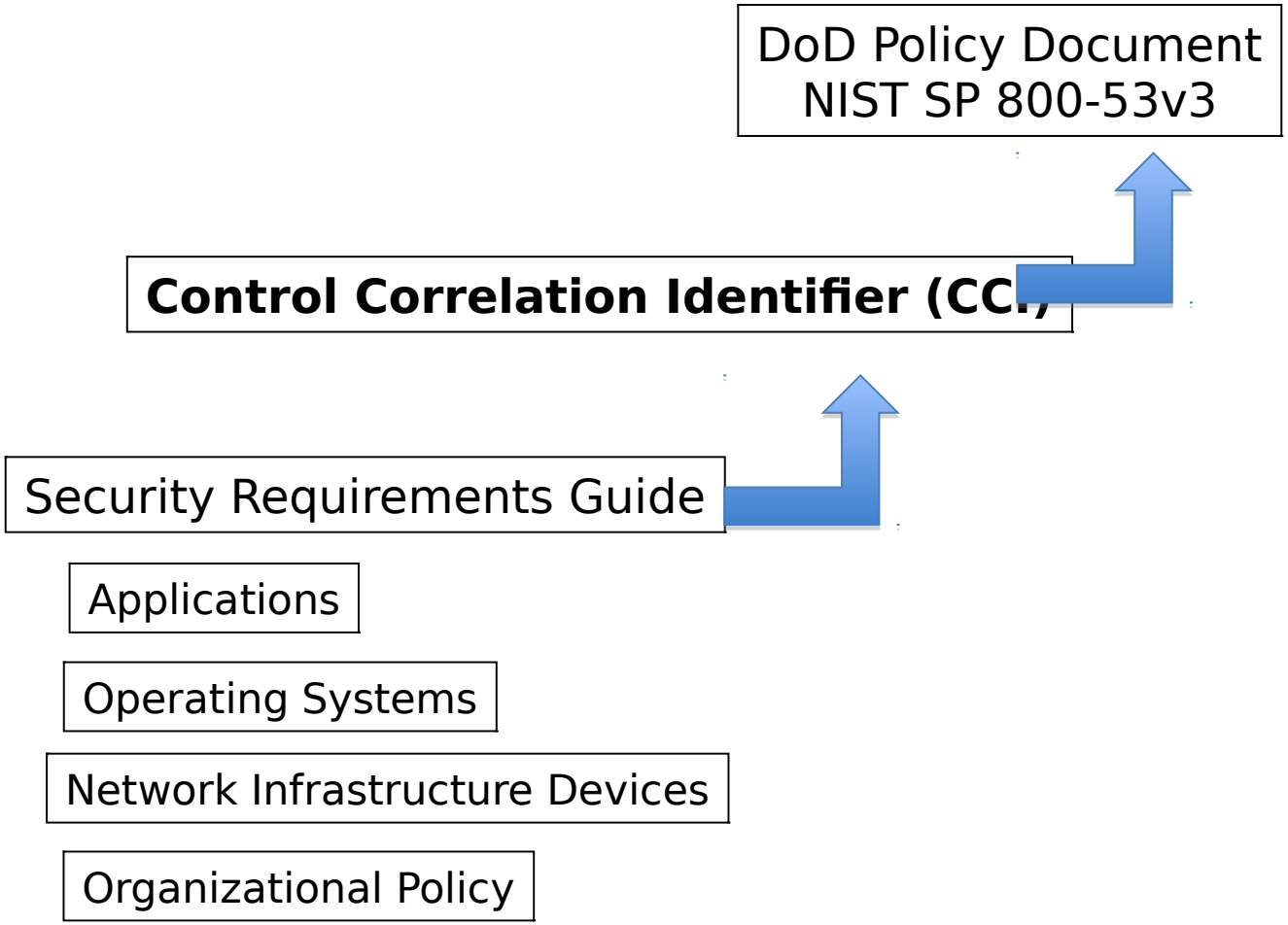
What is an SRG?

Security Requirement Guide:

- A compilation of CCIs
- Requirements grouped into more applicable, specific technology areas
- Documents baselines established by DoD through the CNSS 1253
- Layer to bridge gap between policy, STIGs, and tools
- Provides DoD specificity to CCI requirements
- Non-vendor specific
- No check and fix – just the requirement
- Can be used by guide developers to build STIGs
- Product vendors can use SRG to develop product specific guidance and submit to DoD for validation before being used in C&A process.
- Can be further broken down into technology SRGs

A Combat Support Agency

Requirements Guides & CCI



DISA
A Combat Support Agency

Security Requirements Guide (SRG)

- **Efforts begin in 2010 and will continue**
  - Used UNIX STIG (UNIX SRG Profile) update to flesh out process/concept
  - Planned for FY11
    - Network SRG
    - Operating System SRG
    - Application SRG
    - Policy SRG
- **Will be expressed in XCCDF to automate the generation of guidance documents (SRG and STIGs)**
- **A method to convey additional technology specific details about the CCIs to product vendors by using SRG Baselines**
- **Provides the necessary details or values (organizationally defined parameters)**
- **SRG not intended for use for assessments, STIGs will be used for assessments**

Process Changes

DISA
A Combat Support Agency

DoD Policy

- DoD 8500 Series
- IAVMs
- CTO's
- SP 800-53 & CNSS 1253
- CJCSM & more…

Product Family

- Operating Systems
- Applications
- Network Infrastructure
- Non-Computing & Policy
- Additional Requirements Child SRGs

Analyze Policies ONCE For Each Product Family to Identify Requirements and Implementation Guidance

- 4 SRGs
- Additional SRG
- Unlimited STIGs
- 45,000+ vulnerabilities and requirements in VMS

Publish Guidance

Security Requirement Guides And **STIGs**

Status

- **High Demand for New & Updated Security Guidance**
- **Automated Process to Author Guidance**
- **Define Requirements once, Use them many times**
- **Saves Time and Allows for better Resource Utilization**

A Combat Support Agency

Draft SRGs

- Overview “TIM” was held on 28 Jun 11
- High interest/attendance
- Network and Application SRGs – comment period over 12 Jul
- Policy SRG (Pt 1) and OS SRG – comments due early August
- Working with NSA to map Network SRG to Network Device PP

A Combat Support Agency

Requirements → SRGs

CCI List

CCI-000213: The organization enforces minimum password length.
CCI-000197: The organization enforces password complexity by the number of special characters used.
CCI-000188: The organization manages information system authenticators for users and devices by establishing the time period for changing/refreshing authenticators.
CCI-000186: The organization manages information system authenticators for users and devices by establishing maximum lifetime restrictions for authenticators (if appropriate).
CCI-xxxxxx: …….

Operating System SRG

•CCI-000213: The organization enforces minimum password length.
•CCI-000197: The organization enforces password complexity by the number of special characters used.
•CCI-000188: The organization manages information system authenticators for users and devices by establishing the time period for changing/refreshing authenticators.
•CCI-000186: The organization manages information system authenticators for users and devices by establishing maximum lifetime restrictions for authenticators (if appropriate).
•CCI-xxxxxx:
……

Network SRG

•CCI-000213: The organization enforces minimum password length.
•CCI-000197: The organization enforces password complexity by the number of special characters used.
•CCI-000188: The organization manages information system authenticators for users and devices by establishing the time period for changing/refreshing authenticators.
•CCI-000186: The organization manages information system authenticators for users and devices by establishing maximum lifetime restrictions for authenticators (if appropriate).
•CCI-xxxxxx:
……

Application SRG

•CCI-000213: The organization enforces minimum password length.
•CCI-000197: The organization enforces password complexity by the number of special characters used.
•CCI-000188: The organization manages information system authenticators for users and devices by establishing the time period for changing/refreshing authenticators.
•CCI-000186: The organization manages information system authenticators for users and devices by establishing maximum lifetime restrictions for authenticators (if appropriate).
•CCI-xxxxxx:
……

Policy SRG

•CCI-000213: The organization defines minimum password length.
•CCI-000197: The organization defines password complexity by the number of special characters used.
•CCI-000188: The organization defines information system authenticators for users and devices by establishing the time period for changing/refreshing authenticators.
•CCI-000186: The organization defines information system authenticators for users and devices by establishing maximum lifetime restrictions for authenticators (if appropriate).
•CCI-xxxxxx:
……

A Combat Support Agency

Requirements → SRGs

Operating System SRG

•CCI-000213: The organization enforces minimum password length.
•CCI-000197: The organization enforces password complexity by the number of special characters used.
•CCI-000188: The organization manages information system authenticators for users and devices by establishing the time period for changing/refreshing authenticators.
•CCI-000186: The organization manages information system authenticators for users and devices by establishing maximum lifetime restrictions for authenticators (if appropriate).
•CCI-xxxxxx: .....

Network SRG

•CCI-000213: The organization enforces minimum password length.
•CCI-000197: The organization enforces password complexity by the number of special characters used.
•CCI-000188: The organization manages information system authenticators for users and devices by establishing the time period for changing/refreshing authenticators.
•CCI-000186: The organization manages information system authenticators for users and devices by establishing maximum lifetime restrictions for authenticators (if appropriate).
•CCI-xxxxxx: .....

Application SRG

•CCI-000213: The organization enforces minimum password length.
•CCI-000197: The organization enforces password complexity by the number of special characters used.
•CCI-000188: The organization manages information system authenticators for users and devices by establishing the time period for changing/refreshing authenticators.
•CCI-000186: The organization manages information system authenticators for users and devices by establishing maximum lifetime restrictions for authenticators (if appropriate).
•CCI-xxxxxx: .....

Policy SRG

•CCI-000213: The organization defines minimum password length.
•CCI-000197: The organization defines password complexity by the number of special characters used.
•CCI-000188: The organization defines information system authenticators for users and devices by establishing the time period for changing/refreshing authenticators.
•CCI-000186: The organization defines information system authenticators for users and devices by establishing maximum lifetime restrictions for authenticators (if appropriate).
•CCI-xxxxxx: .....

Database SRG

•CCI-000213: The organization enforces minimum password length.
•CCI-000197: The organization enforces password complexity by the number of special characters used.
•CCI-000188: The organization manages information system authenticators for users and devices by establishing the time period for changing/refreshing authenticators.
•CCI-000186: The organization manages information system authenticators for users and devices by establishing maximum lifetime restrictions for authenticators (if appropriate).
•CCI-xxxxxx:
.....

Web Server SRG

•CCI-000213: The organization enforces minimum password length.
•CCI-000197: The organization enforces password complexity by the number of special characters used.
•CCI-000188: The organization manages information system authenticators for users and devices by establishing the time period for changing/refreshing authenticators.
•CCI-000186: The organization manages information system authenticators for users and devices by establishing maximum lifetime restrictions for authenticators (if appropriate).
•CCI-xxxxxx:
.....

eMail Server SRG

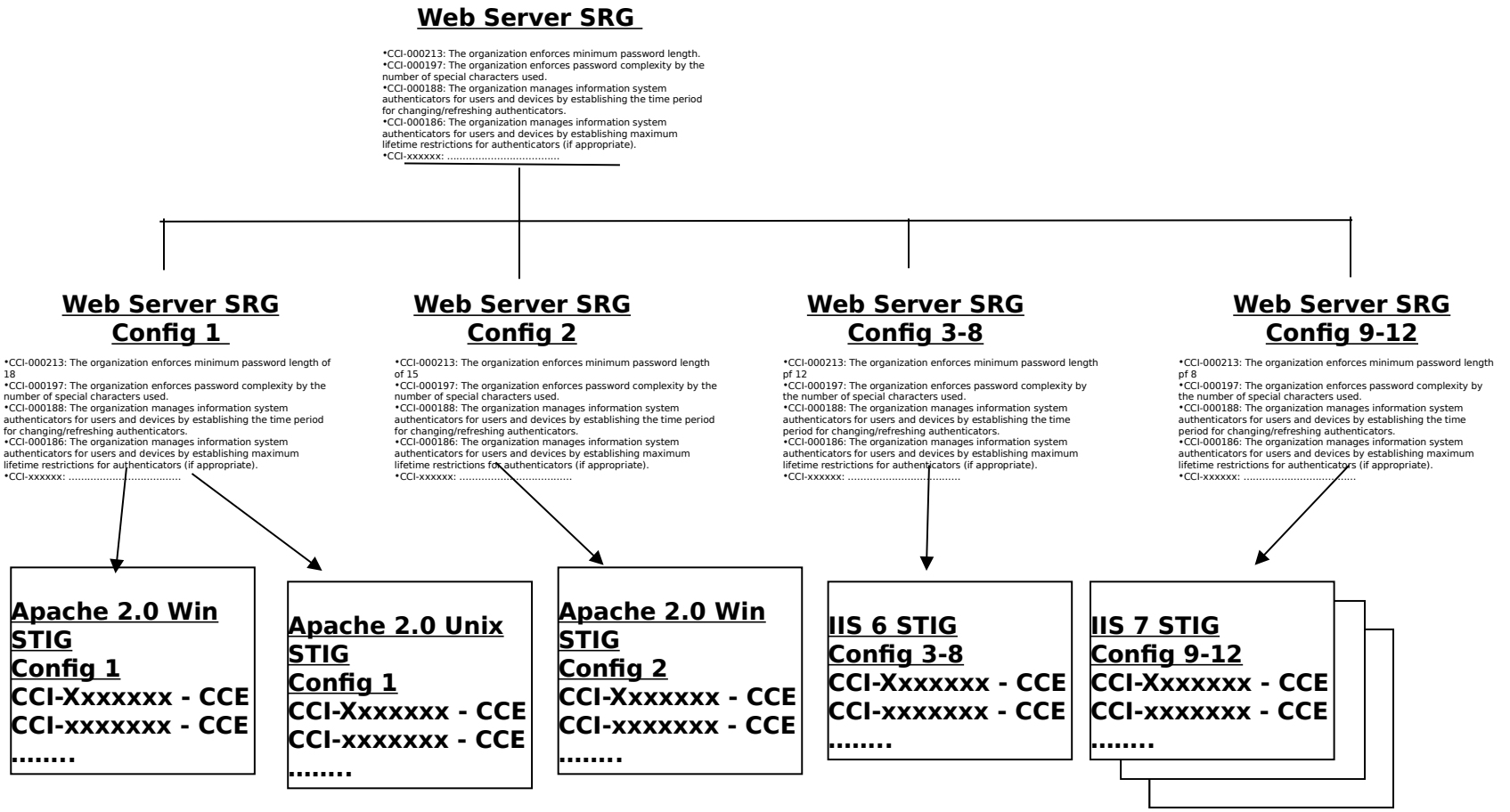
•CCI-000213: The organization enforces minimum password length.
•CCI-000197: The organization enforces password complexity by the number of special characters used.
•CCI-000188: The organization manages information system authenticators for users and devices by establishing the time period for changing/refreshing authenticators.
•CCI-000186: The organization manages information system authenticators for users and devices by establishing maximum lifetime restrictions for authenticators (if appropriate).
•CCI-xxxxxx:
.....

App Server SRG

•CCI-000213: The organization defines minimum password length.
•CCI-000197: The organization defines password complexity by the number of special characters used.
•CCI-000188: The organization defines information system authenticators for users and devices by establishing the time period for changing/refreshing authenticators.
•CCI-000186: The organization defines information system authenticators for users and devices by establishing maximum lifetime restrictions for authenticators (if appropriate).
•CCI-xxxxxx:
.....

Technology SRGs > Configs

A Combat Support Agency



STIGs contain the Product Specific Check and Fix Information

A Combat Support Agency

Applying Technology SRGs > Assets

Windows 2003 IIS 6 Web Server
Web Site1
Web Site 2
Web Site 3

Config 2

IIS 6 STIG Config 2

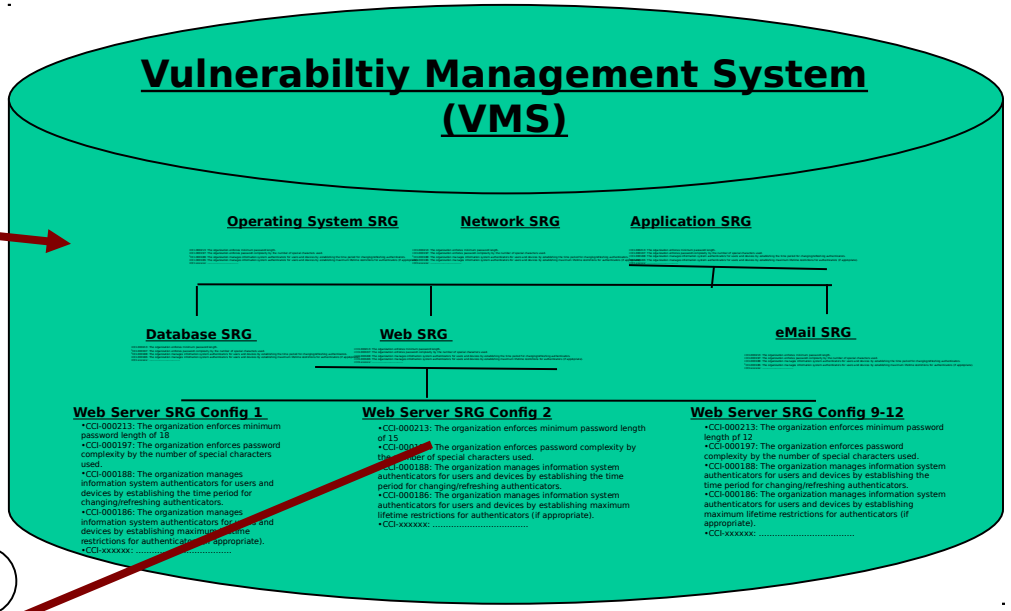
- CCI-000213: The organization enforces minimum password length of 15 – CCE000
- CCI-000186: The organization manages information system authenticators for users and devices by establishing maximum lifetime restrictions for authenticators (if appropriate). – CCE001
- CCI-xxxxxx: .....

Windows 2003 STIG Config 2

- CCI-000213: The organization enforces minimum password length of 15 – CCE099
- CCI-000186: The organization manages information system authenticators for users and devices by establishing maximum lifetime restrictions for authenticators (if appropriate). – CCE187
- CCI-xxxxxx: .....

1

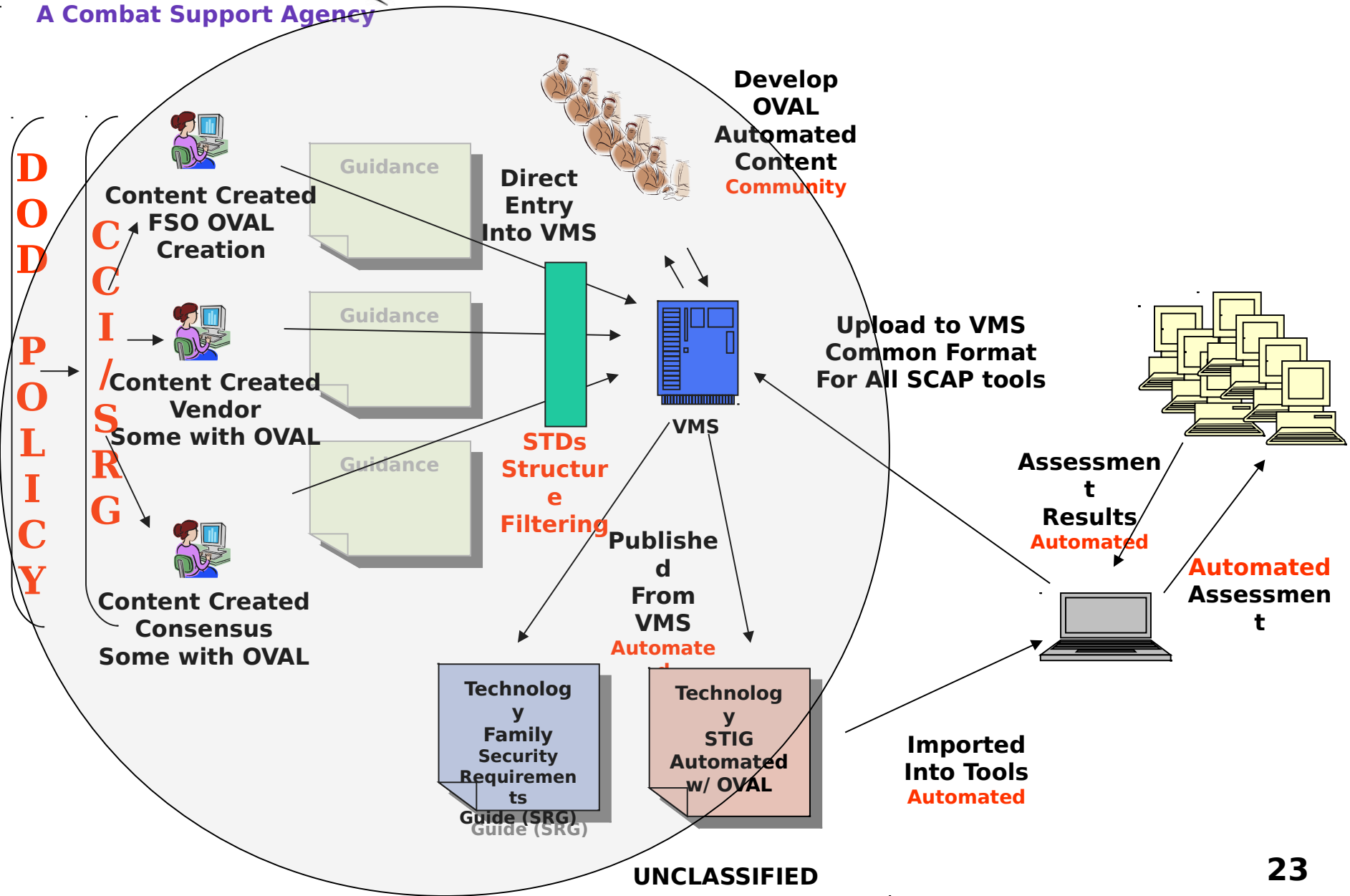
2



1. **Apply Asset Posture to VMS CCI / SRG / Technology SRG Information**
2. **VMS Returns Asset Specific Requirements based on Technologies and Configurations**

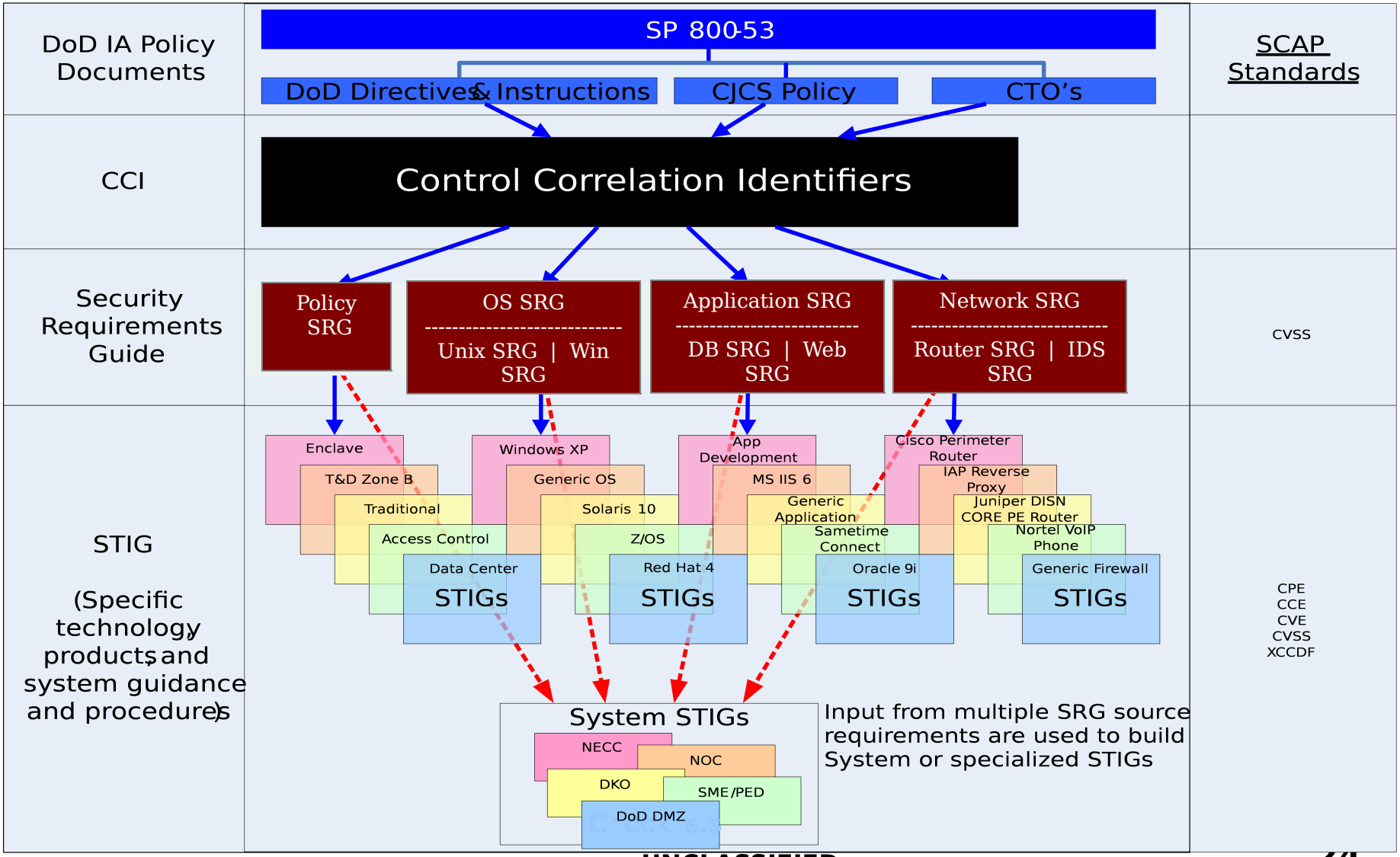
STIG Automation Way Ahead

A Combat Support Agency



DISA
A Combat Support Agency

Future



DISA
A Combat Support Agency

Automation Status: Windows

- **Automated Benchmarks (with OVAL) available for the following Windows platforms:**
  - **Windows XP**
  - **Windows Vista**
  - **Windows 2003 Domain Controller & Member Server**
  - **Windows 2008 Domain Controller & Member Server**
  - **Windows 7 (August release)**
- **Windows STIGs published in XCCDF for:**
  - **Windows 2003**
  - **Windows 2008**
  - **Windows XP**
  - **Windows Vista**
  - **Windows 7**

DISA
A Combat Support Agency

Automation Status: UNIX

- **OS SRG UNIX Published 19 Nov 2010**
- **Automated Benchmarks (with OVAL) will be available for the following UNIX platforms by end of CY11:**
  - **Red Hat 4**
  - **Red Hat 5**
  - **Solaris 9**
  - **Solaris 10**
  - **HP-UX 11.23**
  - **HP-UX 11.31**
  - **AIX 5.3**
  - **AIX 6.1**
- **UNIX STIGs in XCCDF for all versions of UNIX**

DISA
A Combat Support Agency

Future

- As SCAP evolves
  - Use of SCAP Benchmarks for Assessments
  - Use of IAVM Benchmarks for Patch Validation
  - Phase out of Gold Disk
  - Phase out of UNIX Scripts

DISA
A Combat Support Agency

Questions ?

Discussion

DISA
A Combat Support Agency

Security Content Automation Protocol

- **CVE® - Common Vulnerabilities and Exposures**
  - Common naming of emerging vulnerabilities
- **CCE™ - Common Configuration Enumeration**
  - Common naming of configuration (STIG) vulnerabilities
- **CPE™ - Common Platform Enumeration**
  - Language to describe Operating Systems/Platforms
- **CVSS - Common Vulnerability Scoring System**
  - Scoring System to describe severity of a vulnerability
- **XCCDF - Extensible Configuration Checklist Description Format**
  - XML definition of a checklist
- **OVAL™ - Open Vulnerability and Assessment Language**
  - Common language for assessing status of a vulnerability

- **CCI – Control Correlation Identifiers**
  - Common identifier for policy based requirements
  - Currently not under SCAP umbrella, but within the Framework

- **Data sources maintained in and published from National Vulnerability Database (NVD)**